City of Milwaukee

DEPARTMENT OF EMPLOYEE RELATIONS
ATTENTION CITY OF MILWAUKEE EMPLOYEES
IMPORTANT INFORMATION ABOUT IDENTITY THEFT PROTECTION

In response to the incident reported to the City of Milwaukee on November 15th involving Dynacare Laboratories, the Department of Employee Relations is working to investigate and determine the full circumstances underlying this incident and pursue appropriate corrective measures. A dedicated line has been established by Dynacare for City employees who have questions about the incident. The number is 1-877-237-4971, Monday - Friday, 9:00 am to 5:00pm.

All City employees will be receiving a letter from Dynacare Laboratories with information about an offer of one-year free membership in "ProtectMyID Alert" an identity theft notification program. The letter will contain instructions on how to activate your complimentary membership. The City recommends you take advantage of this offer as it may help detect, protect, and resolve potential identity theft.

The following information summarizes other steps you may take to protect yourself from identity theft.

1. Place an Initial Fraud Alert

Three national credit reporting companies keep records of your credit history. If your personal information is compromised, call one of the companies and ask for an initial fraud alert on your credit report. A fraud alert is free. You must provide proof of your identity. The company you call must tell the other companies about your alert. An initial fraud alert can make it harder for an identity thief to open accounts in your name. When you have an alert on your report, a business must verify your identity before it issues credit, so it may try to contact you. The initial alert stays on your report for at least 90 days. You can renew it after 90 days. It allows you to order one free copy of your credit report from each of the three credit reporting companies. Be sure the credit reporting companies have your current contact information so they can get in touch with you.

Credit Reporting Companies:	Equifax	Experian	TransUnion
	1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Order Your Credit Reports

After you place initial fraud alert, you will be entitled to a free credit report from each of the three credit reporting companies. When requesting the credit report, ask the company to show only the last four digits of your Social Security number on your report. When you receive the report, review all accounts and charges to determine if there are any fraudulent transactions. mail and ask for a return receipt to create a record of your communications.

3. Reviewing your Credit Report and Disputing Errors with Credit Reporting Companies

Review your credit reports to see whether fraudulent transactions or accounts are listed. Your credit report contains information about where you live, how you pay your bills, and whether you've been sued or arrested, or have filed for bankruptcy. The information in your credit report is used to evaluate your applications for credit, insurance, employment, and renting a home, so it is important that the information is accurate and up-to-date.

If you see errors in the report, like accounts you didn't open or debts you didn't incur, contact the credit reporting company and the fraud department of each business where an error or fraudulent transaction has been identified. Follow up in writing and send your letters by certified.

4. What to do if you Become a Victim of Identity Theft

Some of the clues or signs that someone has stolen your identity include: you see withdrawals from your bank account that you can't explain, you don't get your bills or other mail, merchants refuse your checks, debt collectors call you about debts that aren't yours, you find unfamiliar accounts or charges on your credit report, medical providers bill you for services you didn't use, your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit, a health plan won't cover you because your medical records show a condition you don't have, the IRS notifies you that more than one tax return was filed in your name or that you have income from an employer you don't work for.

If you think you've become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts. You should create an Identity Theft report to help you deal with credit reporting companies, debt collectors, and businesses that gave the identity thief credit or opened new accounts in your name. You can use the Report to get fraudulent information removed from your credit report, stop a company from collecting debts that result from identity theft, or from selling the debt to another company for

collection, place an extended fraud alert on your credit report, and get information from companies about accounts the identity thief opened or misused.

Instructions on how to create an Identity Theft Report can be found at http://www.consumer.ftc.gov/articles/0277-create-identity-theft-report#How

Here is a list of OTHER ACTIONS that you may want to take right away:

Contact the FEDERAL TRADE COMMISSION to report the situation, 1-877-ID THEFT (877-438-4338) or TDD at 1-866-653-4261. The FTC is responsible for receiving and processing complaints from people who believe they may be victims of identity theft.

Contact your local POST OFFICE if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit fraud involving your identity.

Contact the SOCIAL SECURITY ADMINISTRATION if you suspect that your Social Security number is being fraudulently used.

Contact the INTERNAL REVENUE SERVICE if you suspect the improper use of identification information in connection with tax violations.

Contact the fraud units of the three principal CREDIT REPORTING COMPANIES.

Contact all CREDITORS with whom your name or identifying data have been fraudulently used.

Contact all FINANCIAL INSTITUTIONS where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

Additional information from the Wisconsin Office of Privacy Protection can be found at http://datcp.wi.gov/Consumer/Office_of_Privacy_Protection/